

Maurer School of Law: Indiana University Digital Repository @ Maurer Law

Articles by Maurer Faculty

Faculty Scholarship

2012

The Supreme Court and Information Privacy

Fred H. Cate

Indiana University Maurer School of Law, fcate@indiana.edu

Beth E. Cate

Indiana University - Bloomington, becate@indiana.edu

Follow this and additional works at: <http://www.repository.law.indiana.edu/facpub>



Part of the [Constitutional Law Commons](#), and the [Privacy Law Commons](#)

Recommended Citation

Cate, Fred H. and Cate, Beth E., "The Supreme Court and Information Privacy" (2012). *Articles by Maurer Faculty*. 2614.
<http://www.repository.law.indiana.edu/facpub/2614>

This Editorial is brought to you for free and open access by the Faculty Scholarship at Digital Repository @ Maurer Law. It has been accepted for inclusion in Articles by Maurer Faculty by an authorized administrator of Digital Repository @ Maurer Law. For more information, please contact wattn@indiana.edu.



LAW LIBRARY
INDIANA UNIVERSITY
Maurer School of Law
Bloomington

The Supreme Court and information privacy

Fred H. Cate* and Beth E. Cate**

Introduction

The US Supreme Court has written a great deal about ‘privacy’ in a wide variety of contexts. Between 1970 and 2011, the Court used the term ‘privacy’ in 631 opinions. In just over half (328 opinions) did an opinion significantly address some aspect of privacy.

The breakdown of those 328 opinions offers insight into the contexts in which the Supreme Court concerns itself with privacy (Figure 1). Not surprisingly, most of these opinions addressed privacy rights that the Court has found are protected by the US Constitution. The largest single category by far was cases involving a ‘reasonable expectation of privacy’ under the Fourth Amendment to the Constitution (210, or 64 per cent of opinions), including the extent to which privacy rights are implicated, or violated, by searches or seizures that are initiated or conducted by private parties with some degree of government involvement. Opinions involving the First Amendment and freedom of expression and association issues accounted for 18 per cent (59), a large portion of which involved reviews of obscenity regulations and prosecutions. Fourteen opinions (4 per cent) involved what the Court has come to call ‘decisional privacy’, namely the privacy rights the Court has found implied in the Constitution that protect the rights of adults to make decisions about activities such as reproduction, contraception, the education of their children, and sexual intimacy. A handful of opinions (16, or 5 per cent) involve the privacy-related characteristics of the Fifth Amendment’s protection against self-incrimination.

Aside from constitutional privacy issues, 20 (6 per cent) of the Court’s opinions involving privacy addressed the application of the two privacy exemptions to the Freedom of Information Act. A significant number of opinions (69, or 21 per cent) did not fit neatly within any single discrete category, but reflect a

Abstract

- Advances in technology—including the growing use of cloud computing by individuals, agencies, and organizations to conduct operations and store and process records—are enabling the systematic collection and use of personal data by state and federal governments for a variety of purposes.
- These purposes range from battling crime and terrorism to assessing public policy initiatives and enforcing regulatory regimes. To aid these efforts, governments are promoting mandatory retention and reporting of data by online service providers and the expansion of laws that facilitate wiretaps to greater portions of the web.
- The legal framework for protecting individual privacy within this growing world of ‘big data’ is patchy and in critical ways outdated. Most of the current framework was erected in response to pronouncements by the Supreme Court over the years regarding the scope of constitutional privacy protections. Widespread agreement over the need for legislators to update the statutory regime has not yet produced results.
- Against this backdrop, the US Supreme Court has struggled in recent cases to articulate workable constitutional and statutory privacy norms that can help guide government, and individuals, in a world of digital and distributed data. An examination of the Court’s privacy jurisprudence over the past forty years offers a number of insights into how the Court, and policy-makers, may achieve a balance between privacy and data use that accords with constitutional norms, serves vital public policy goals, and secures greater public trust and support.

* Fred H. Cate, Distinguished Professor and C. Ben Dutton Professor of Law, Maurer School of Law, Indiana University. Email: fred@fredcate.org.

** Beth E. Cate, Associate Professor, School of Public and Environmental Affairs, Indiana University. Email: becate@indiana.edu.

The authors gratefully acknowledge the funding for this paper provided by a grant from The Privacy Projects, <www.theprivacyprojects.org>. Excellent research assistance was provided by Lindsay Elizabeth Koenings.

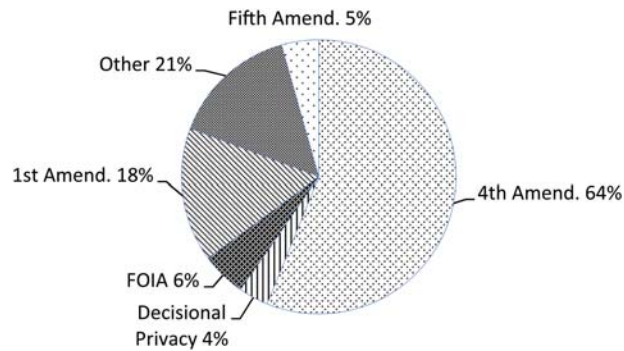


Figure 1 US Supreme Court cases involving privacy, 1970–2011
Note: $n = 328$, total greater than 100% due to double-counting

range of other statutory or common-law issues including statutory privacy rights and common law privacy torts; and evidentiary privileges and rules that reflect privacy or confidentiality norms (such as the attorney–client privilege and attorney work product doctrine). The total number of opinions does not add up to 328 (or the total percentages to 100 per cent) because a number of opinions addressed more than one aspect of privacy.

The breadth of the Court's constitutional privacy jurisprudence reflects the fact that even though privacy is not protected by name in the Constitution, the Supreme Court has interpreted many of the amendments constituting the Bill of Rights to protect various elements of privacy. These include an individual's right to be free from unreasonable searches and seizures by the government;¹ the right to make decisions about issues involving 'fundamental' individual liberty interests such as contraception,² abortion,³ marriage, procreation, child rearing, and sexual intimacy;⁴ the right not to disclose certain information to the government;⁵ the right to associate free from government intrusion;⁶ and the right to enjoy one's own home free from intrusion by the government,⁷ sexually explicit mail⁸ or radio broadcasts,⁹ or others who would disrupt one's solitude.¹⁰

In the pages that follow we provide an overview of the Supreme Court's treatment of privacy, first in its constitutional exposition, and second in its statutory interpretation, with an emphasis on FOIA. We conclude with a brief analysis of the apparent inconsistency within the Court's jurisprudence of what constitutes a 'reasonable expectation' of privacy and some thoughts on where the Court's privacy jurisprudence may be heading in the context of developing norms and policies that shape government access to personal data, particularly sizeable amounts of data in databases maintained by private-sector sources.

Constitutional sources of a privacy right

Fundamental rights in the United States are articulated in the federal Constitution. Two features of those rights are central to understanding the role of the Constitution in protecting privacy. First, rights articulated in the Constitution generally are protected only against government action.¹¹ All constitutional rights—whether to speak freely, confront one's accusers, be tried by a jury of one's peers—regulate the public, but not the private, sector. In the absence of state action, therefore, constitutional rights are not implicated in questions surrounding privacy.¹² The second significant characteristic of constitutional rights is that they are generally 'negative'; they do not obligate the government to do anything, but rather to refrain from taking actions that abridge constitutionally protected rights.

Fundamental rights of personal decision making

The US Supreme Court's most controversial constitutional right to privacy has developed within a series of cases involving decision making about contraception, abortion, and other issues involving intimate or familial relations. Indeed, decisional 'privacy' rights are better thought of, and often characterized by the Court, as rights of personal autonomy.¹³

1 *Katz v United States*, 389 U.S. 347 (1967).

2 *Griswold v Connecticut*, 381 U.S. 479 (1965).

3 *Roe v Wade*, 410 U.S. 113 (1973).

4 *Id.* at 152–3; *Lawrence v Texas*, 539 U.S. 558 (2003).

5 *Whalen v Roe*, 429 U.S. 589 (1977).

6 *NAACP v Alabama*, 357 U.S. 449 (1958).

7 *Stanley v Georgia*, 394 U.S. 557 (1969).

8 *Rowan v Post Office*, 397 U.S. 728 (1970).

9 *Federal Communications Commission v Pacifica Found.*, 438 U.S. 726 (1978).

10 *Frisby v Schultz*, 487 U.S. 474 (1988); *Carey v Brown*, 447 U.S. 455 (1980).

11 Only the Thirteenth Amendment, which prohibits slavery, applies directly to private parties. *Clyatt v United States*, 197 U.S. 207, 216–220 (1905).

12 Although state action is usually found when the state acts toward a private person, the Supreme Court has also found state action when the state affords a legal right to one private party which impinges on the constitutional rights of another, see *New York Times Co. v Sullivan*, 376 U.S. 264, 265 (1964), and in rare cases when a private party undertakes a traditionally public function, see *Marsh v Alabama*, 326 U.S. 501 (1946), or when the activities of the state and a private entity are sufficiently intertwined to render the private parties' activities public, see *Evans v Newton*, 382 U.S. 296 (1966).

13 See *Lawrence v Texas*, 539 U.S. 558 (2003); *Gonzales v Carhart*, 550 U.S. 124, 172 (2007) (Ginsburg, J., dissenting) ('legal challenges to undue restrictions on abortion procedures do not seek to vindicate some

In 1965, the Supreme Court decided in *Griswold v Connecticut* that an 80-year-old Connecticut law forbidding the use of contraceptives violated the constitutional right to ‘marital privacy’.¹⁴ The justices voting to strike down the law identified a variety of constitutional sources for this right. Justice Douglas, writing the opinion for the Court, drew on notions of privacy implied within several provisions of the Bill of Rights:

Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one. . . . The Third Amendment in its prohibition against the quartering of soldiers ‘in any house’ in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the ‘right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.’ The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: ‘The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.’¹⁵

Justice Douglas concluded in a now-famous turn of phrase that the ‘specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance’.¹⁶ Justices Goldberg and White, agreeing that the Connecticut law was invalid, focused on the Ninth Amendment and wrote that the autonomy of married couples to decide whether or not to have children was a fundamental and traditional right retained by the people. Justice Harlan’s concurrence grounded the privacy right in the Due Process Clause of the Fourteenth Amendment,¹⁷ which he believed protected certain ‘values implicit in the concept of ordered liberty’, among them the right of married couples to engage in contraception without interference by the government.

Justice Harlan’s reliance on the Due Process Clause emerged in subsequent cases as the dominant view of the constitutional basis for decisional privacy rights. Most controversially, eight years after *Griswold*, the Court, in *Roe v Wade*, recognized a constitutional privacy right, grounded in Due Process, that encompasses ‘a woman’s decision whether or not to terminate her pregnancy’.¹⁸ The Court looked to ‘the Fourteenth Amendment’s concept of personal liberty and restrictions upon state action . . .’¹⁹ To guard against the potential for justices to greatly limit the scope of permissible legislative action by transforming their own policy preferences into constitutionally protected “liberties,” the Court in *Roe v Wade* emphasized that the constitutional ‘guarantee of personal privacy’ only includes ‘personal rights that can be deemed “fundamental” or “implicit in the concept of ordered liberty” . . .’²⁰ The Court specified that those fundamental rights include activities concerning marriage, procreation, contraception, family relationships, and child rearing and education.²¹ Government regulation of those activities ‘may be justified only by a “compelling state interest”’, and they must be ‘narrowly drawn to express only the legitimate state interests at stake’²²—a standard described as ‘strict scrutiny’.

Although the Supreme Court indicated that government intrusion into inherently private areas of personal life would be subject to strict scrutiny, the Court over time has come to apply a lesser form of scrutiny to regulations involving abortion, and to emphasize the importance of balancing privacy with the government’s valid regulatory interests.²³ Currently regulations imposed on pregnant women seeking abortions prior to fetal viability will be upheld as long as they do not impose an ‘undue burden’ on access to abortion.²⁴ Similarly, in *Lawrence v Texas*,²⁵ the Court held that a state law criminalizing private sexual conduct between consenting same sex couples failed to pass muster

generalized notion of privacy; rather, they center on a woman’s autonomy to determine her life’s course, and thus to enjoy equal citizenship stature’.)

14 *Griswold v Connecticut*, 381 U.S. 479 (1965). The Court later extended constitutional rights of access to contraception to unmarried individuals, see *Eisenstadt v Baird*, 405 U.S. 438, 453 (1972) (‘[i]f the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether or not to bear or beget a child’).

15 *Id.* at 484.

16 *Id.*

17 The Fourteenth Amendment provides, in relevant part: ‘No State shall make or enforce any law which shall . . . deprive any person of life, liberty, or property, without due process of law . . .’ US Constitution amend. XIV. The Fifth Amendment applies an identical prohibition to the federal government. US Constitution amend. V.

18 410 U.S. 113, 153 (1973).

19 *Id.*

20 *Roe v Wade*, 410 U.S. at 152 (quoting *Palko v Connecticut*, 302 U.S. 319, 325 (1937)).

21 *Id.* at 152–3.

22 *Id.* at 155.

23 *Planned Parenthood of Southeastern Pennsylvania v Casey*, 505 U.S. 833 (1992).

24 *Id.* After viability a state’s interest in preserving the potentiality of the life of the fetus outweighs the mother’s privacy rights and the state may ban abortion altogether except when needed to save the life or protect the health of the mother. *Stenberg v Carhart*, 530 US 914 (2000). But see *Gonzales v Carhart* (n 13) (rejecting facial challenge to federal Partial-Birth Abortion Act of 2003, which does not contain an exception to the ban on partial-birth abortions to protect a woman’s health, but not ruling out challenges to individual applications of the law).

25 539 U.S. 558.

under the Due Process Clause. Although restating that the freedom to make intimate personal choices is central to the liberty protected by Due Process, the Court ultimately employed a much lower standard of review than strict scrutiny and found that the state law was not rationally related to furthering any legitimate government interest.²⁶

The Court's decisional privacy jurisprudence generally does not concern issues of informational privacy. In the abortion context, however, the Court has addressed certain rules that implicate informational privacy concerns. For a number of years following *Roe v Wade*, the Court struck down state laws that required pregnant women, including minors, to obtain spousal or parental consent to abortion (at least in the absence of an alternative when parental consent is unavailable or inappropriate),²⁷ and also struck down rules requiring women to receive information about risks and alternatives that the Court found to be designed to deter a woman from having an abortion.²⁸ In 1992, however, the Court upheld a requirement that abortion patients receive an 'informed consent' booklet with information on risks and alternatives, a 24-hour waiting period, and a requirement that minors get the written consent of at least one parent, finding that none of these requirements unduly interfered with the right to access abortion.²⁹ In doing so, the Court signalled its willingness to balance individual information privacy rights with other firmly held policy values.

Protection against Government-compelled disclosure of personal matters

In addition to weighing the privacy issues raised by compelled disclosures in the abortion setting, the

Supreme Court has addressed privacy in the context of a more general constitutional right against government-compelled 'disclosure of personal matters'.³⁰ In 1977, the Supreme Court decided *Whalen v Roe*, a case involving a challenge to a New York statute requiring that copies of prescriptions for certain 'scheduled' (lawful but dangerous) drugs be provided to the state. The state enacted the statute to combat overprescription of drugs that were making their way into an illegal market; patients, doctors, and physician associations challenged the law on the basis that the requirement would infringe patients' privacy rights. Echoing *Griswold*, the unanimous Court wrote that the constitutionally protected 'zone of privacy' included 'the individual interest in avoiding disclosure of personal matters'.³¹

Nevertheless, having found this new privacy interest in the non-disclosure of personal information, the Court did not apply strict scrutiny, a standard typically reserved for cases involving 'fundamental' interests. Instead, applying a lower level of scrutiny, the Court found that the statute did not infringe the individuals' interest in non-disclosure.³² The Court also explicitly rejected the application of the Fourth Amendment right of privacy to broad government data collection programmes for regulatory purposes, writing that Fourth Amendment cases 'involve affirmative, unannounced, narrowly focused intrusions'.³³ The Supreme Court has never decided a case in which it found that a government regulation or action violated the constitutional privacy right recognized in *Whalen*.³⁴

Yet the Court in *Whalen* provided a comparatively subtle and modern understanding of what 'privacy' means:

interest against the strong public interest in preserving presidential papers and the extensive procedural protections against unwarranted disclosure of private information, and concluding that the archival requirements were reasonable and thus constitutional. Id. at 455–65. The more direct reliance on Fourth Amendment principles to resolve the privacy claims is perhaps unsurprising given that the law in question applied only to the Nixon presidential records and no others.

34 Several federal appeals courts have relied on *Whalen*, however, to find that a government regulation or action violated an individual's constitutional privacy right in nondisclosure of personal information. See, eg *Tavoulareas v Washington Post Co.*, 724 F.2d 1010 (D.C. Cir. 1984); *Barry v City of New York*, 712 F.2d 1554 (2d Cir. 1983); *Schacter v Whalen*, 581 F.2d 35 (2d Cir. 1978); *Doe v Southeastern Pennsylvania Transportation Authority*, 72 F.3d 1133 (3d Cir. 1995); *United States v Westinghouse Electric Corp.*, 638 F.2d 570 (3d Cir. 1980); *Plante v Gonzalez*, 575 F.2d 1119 (5th Cir. 1978), and *Doe v Attorney General*, 941 F.2d 780 (9th Cir. 1991). Courts in the Fourth and Sixth Circuits, in contrast, have severely limited the scope of the *Whalen* nondisclosure privacy right, see *Walls v City of Petersburg*, 895 F.2d 188, 192 (4th Cir. 1990), and *J.P. v DeSanti*, 653 F.2d 1080 (6th Cir. 1981). Taking *Whalen's* lead, those courts that have relied on the right of nondisclosure have applied only intermediate scrutiny, instead of the

26 Id. at 573–4, 577–8.

27 Eg *Planned Parenthood of Central Missouri v Danforth*, 428 U.S. 52 (1976); *Bellotti v Baird*, 443 U.S. 622 (1979); *City of Akron v Akron Center for Reproductive Health*, 462 U.S. 416 (1983).

28 *Akron* (n 27); *Thornburgh v American College of Obstetricians & Gynecologists*, 476 U.S. 747 (1986).

29 *Casey*, 505 U.S. 833.

30 *Whalen v Roe*, 429 U.S. 589, 599–600 (1977).

31 Id. at 599–600.

32 Id. at 603–4.

33 Id. at 604, n.32. In *Nixon v Administrator of General Services*, 433 U.S. 425 (1977), the Court rejected claims by President Nixon that privacy rights under the Fourth and Fifth Amendments were violated by the Presidential Recordings and Materials Preservation Act, which required him to provide his presidential papers and recordings for archiving, with purely private and personal materials being returned to him. The Court quoted *Whalen* in support of a constitutional-level 'individual interest in avoiding disclosure of personal matters', and like *Whalen* employed a balancing test to determine ultimately the 'reasonableness' of the government's data collection. Unlike *Whalen*, the *Nixon* Court conducted the balancing test in Fourth Amendment terms: finding a limited expectation of privacy in the materials at issue, weighing that

We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures.³⁵

The Court recognized that ‘in some circumstances that duty [to avoid unwarranted disclosures] arguably has its roots in the Constitution.’³⁶ The New York statute did not violate the Constitution, the Court concluded, because it ‘evidence[d] a proper concern with, and protection of, the individual’s interest in privacy’ by authorizing limited access to the data reported and requiring physical and electronic security measures to protect against unauthorized access.³⁷ The Court concluded: ‘We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data—whether intentional or unintentional—or by a system that did not contain comparable security provisions.’³⁸

In *NASA v. Nelson*,³⁹ a six-justice majority of the Court essentially hewed to *Whalen*’s analysis in rejecting a constitutional privacy challenge to certain questions included in an agency’s background check procedure for contract employees. The *Nelson* Court weighed the competing interests of the agency (this time, as an employer rather than a regulator) and its personnel in obtaining and withholding, respectively, information about current drug use treatment and counselling and other information that may bear on an employee’s suitability for employment, using a ‘reasonableness’ standard. Two factors substantially influenced the Court’s conclusion that the data collection was reasonable and lawful: the fact that public and private

employers widely use such background checks, and, as in *Whalen*, the existence of statutory protections (this time, under the federal Privacy Act) against public disclosure of the information collected. The Court rejected arguments that the drug treatment and suitability data were exposed to unreasonable risks from Privacy Act exemptions permitting disclosures of personal information for ‘routine uses,’ or evidence of a significant number of prior government data breaches (788 at 17 agencies in three years). The Court stated that the ‘mere possibility that security measures will fail provides no “proper ground” for a broad-based attack on government information-collection practices,’ and emphasized the limited nature of the actual ‘routine uses’ of background check data made by NASA.⁴⁰

Notably, the Court assumed, without deciding, the existence of *Whalen*’s constitutional privacy ‘interest in avoiding disclosure of personal matters’ to the government, suggesting that the Court might revisit that premise in a future case.⁴¹ Justices Scalia and Thomas declared in concurring opinions that ‘[a] federal constitutional right to “informational privacy” does not exist’ and ‘the Constitution does not protect a right to informational privacy.’⁴²

First Amendment

The Court has identified a number of privacy interests implicit in the First Amendment.⁴³ For example, in *NAACP v. Alabama*,⁴⁴ the Court struck down an Alabama ordinance requiring the NAACP to disclose its membership lists, finding that such a requirement was an unconstitutional infringement on NAACP members’ First Amendment right of association.⁴⁵ And in *Stanley v. Georgia*,⁴⁶ the Court explicitly linked privacy and free expression by identifying the mutual interests they serve. The Court overturned a conviction under Georgia law for possessing obscene material in the home. While the ‘[s]tates retain broad power to regulate obscenity,’ Justice Marshall wrote for the unanimous Court, ‘that power simply does not extend to mere possession by the

strict scrutiny typically used to protect fundamental constitutional rights. See *Doe v. Attorney General*, 941 F.2d at 796.

35 Id. at 605.

36 Id.

37 Id.

38 Id. at 605–6. As discussed further below, the federal Privacy Act of 1974, 5 U.S.C. §§552a (2010), sets out certain statutory (as distinct from constitutional) limits on disclosure of personal information within federal agency databases, although as with other statutory privacy protections, exemptions to these limits are a mile wide and are likely to impose few meaningful constraints on data sharing and use in the efforts (law enforcement, counterterrorism, regulatory compliance) described above.

39 562 U.S. ___ (2011).

40 Id. at __.

41 The majority declined to reach the issue because the parties and amici had not briefed or fully addressed it. Id. at __ n.10.

42 Id. at __ (Scalia, J., concurring in judgment); id. at __ (Thomas, J., concurring in judgment). Justice Kagan did not participate in the consideration of the case or decision.

43 ‘Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceable to assemble . . .’ U.S. Constitution amend. I.

44 357 U.S. 449 (1958).

45 Id. at 464–65.

46 394 U.S. 557 (1969).

individual in the privacy of his own home'.⁴⁷ The Court based its decision squarely on the First Amendment, which the Court found included the 'right to be free, except in very limited circumstances, from unwanted governmental intrusion into one's privacy'.⁴⁸

More often, however, the Court identifies privacy as an interest in tension with the First Amendment's protection for freedom of expression and press. In *Breard v City of Alexandria*,⁴⁹ for example, the Court upheld an ordinance prohibiting solicitation of private residences without prior permission. The Court found in the First Amendment's free speech guarantee an implicit balance between 'some householders' desire for privacy and the publisher's right to distribute publications in the precise way that those soliciting for him think brings the best results.⁵⁰

The Court has invoked this same implied balancing test in numerous other cases. In *Kovacs v Cooper*,⁵¹ the Court upheld a Trenton, New Jersey ordinance prohibiting the use of sound trucks and loudspeakers:

[t]he unwilling listener is not like the passer-by who may be offered a pamphlet in the street but cannot be made to take it. In his home or on the street he is practically helpless to escape this interference with his privacy by loudspeakers except through the protection of the municipality.⁵²

In *Rowan v U.S. Post Office*,⁵³ the Court upheld a federal statute which permitted homeowners to specify that the Post Office not deliver to their homes 'erotically arousing' and 'sexually provocative' mail. In *Federal Communications Commission v Pacifica Foundation*,⁵⁴ the Court allowed the Federal Communications Commission to sanction a radio station for broadcasting 'indecent' programming, finding that 'the individual's right to be left alone plainly outweighs the First Amendment rights of an intruder'.⁵⁵ In *Frisby v Schultz*,⁵⁶ the Court upheld a local ordinance that

banned all residential picketing, writing that the home was 'the one retreat to which men and women can repair to escape from the tribulations of their daily pursuits'⁵⁷ and 'the last citadel of the tired, the weary, and the sick'.⁵⁸ In *Carey v Brown*,⁵⁹ the Court wrote that 'the State's interest in protecting the well-being, tranquility, and privacy of the home is certainly of the highest order in a free and civilized society'.⁶⁰

When privacy rights conflict with free expression rights before the Court, the latter usually prevail. When information is true and obtained lawfully, the Court has repeatedly held that the state may not restrict its publication without showing a very closely tailored, compelling governmental interest. Under this requirement, the Court has struck down laws restricting the publication of confidential government reports,⁶¹ and of the names of judges under investigation,⁶² juvenile suspects,⁶³ and rape victims.⁶⁴ Moreover, there can be no recovery for invasion of privacy unless the information published is highly offensive to a reasonable person and either false⁶⁵ or not newsworthy.⁶⁶ And the Court has accorded a variety of procedural protections to all expression, whether true or false.⁶⁷

The Court recently revisited the balance between freedom of expression and privacy in *Sorrell v IMS Health Inc.*⁶⁸ *Sorrell* involved a First Amendment challenge to a Vermont law prohibiting the sale, disclosure, or use of prescriber-identifiable information in pharmacy and related records for use in marketing or promoting prescription drugs. The law was aimed at combating expensive, targeted 'detailing' campaigns by drug representatives using prescribed-specific data obtained from pharmacies, insurers, and so on via data mining companies; the state also argued, however, that the law was designed to safeguard prescriber privacy.⁶⁹

Justice Kennedy, writing for the six-justice majority, assumed that 'for many reasons, physicians have an

47 Id. at 568.

48 Id. at 564.

49 341 U.S. 622 (1951).

50 Id. at 644.

51 336 U.S. 77 (1949).

52 Id. at 86–87.

53 397 U.S. 728 (1970).

54 438 U.S. 726 (1978).

55 Id. at 748.

56 487 U.S. 474 (1988).

57 Id. at 484 (quoting *Carey*, 447 U.S. at 455).

58 Id. (quoting *Gregory v City of Chicago*, 394 U.S. 111, 125 (1969) (Black, J., concurring)).

59 447 U.S. 455 (1980). The Court in *Carey* struck down an Illinois ordinance which generally prohibited residential picketing but permitted certain labour picketing; the Court rejected the state's argument that the law properly balanced privacy interests with special solicitude for

labour-related speech, emphasizing that picketing rules designed to protect privacy should be drawn without regard to the content of the speech. Id. at 470–71.

60 Id. at 471.

61 *New York Times Co. v United States*, 403 U.S. 713 (1971).

62 *Landmark Communications, Inc. v Virginia*, 435 U.S. 829 (1978).

63 *Smith v Daily Mail Publishing Co.*, 443 U.S. 97 (1979).

64 *Florida Star v B.J.F.*, 491 U.S. 524 (1989); *Cox Broadcasting Corp. v Cohn*, 420 U.S. 469 (1975).

65 *Cantrell v Forest City Publishing Co.*, 419 U.S. 245 (1974).

66 *Florida Star*, 491 U.S. 254.

67 *Anderson v Liberty Lobby, Inc.*, 477 U.S. 242 (1986) (requiring that the standard for summary judgment motions take into account the plaintiff's burden at trial); *Bose Corp. v Consumers Union*, 466 U.S. 485 (1984) (requiring independent appellate review).

68 564 U.S. ___ (2011).

69 No patient-identifiable information was involved in the disclosures.

interest in keeping their prescription decisions confidential', and strongly suggested that a state law that closely guarded the confidentiality of such information and allowed its disclosure and use 'in only a few narrow and well justified circumstances' would be upheld against the type of challenge brought by the pharmaceutical companies.⁷⁰ The majority concluded, however, that prescriber data were widely available without prescriber consent to others, including 'counterdetailers' promoting non-prescription drugs, and therefore the law was insufficiently tailored to serve its stated privacy goals.⁷¹

Strikingly, though, Justice Kennedy ended the majority opinion with a strong statement—one that echoes to some extent the concluding observations in *Whalen*, above—about the importance of privacy and the risks posed to it by technology-enabled access to and use of personal data held by the government or elsewhere:

The capacity of technology to find and publish personal information, including records required by the government, presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure. In considering how to protect those interests, however, the State cannot engage in content-based discrimination to advance its own side of a debate.

If Vermont's statute provided that prescriber-identifying information could not be sold or disclosed except in narrow circumstances then the State might have a stronger position. Here, however, the State gives possessors of the information broad discretion and wide latitude in disclosing the information, while at the same time restricting the information's use by some speakers and for some purposes, even while the State itself can use the information to counter the speech it seeks to suppress. *Privacy is a concept too integral to the person and a right too essential to freedom to allow its manipulation to support just those ideas the government prefers.*⁷²

Fourth Amendment

One of the colonists' most potent grievances against the British government was its use of general searches. The hostility to general searches found powerful expression in the Fourth Amendment:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.⁷³

Framework

The Fourth Amendment does not purport to keep the government from conducting searches or seizing personal information. It only prohibits 'unreasonable' searches and seizures, but is silent about what makes a search or seizure 'unreasonable'. In 1886, the Supreme Court first applied the term 'priva[cy]' to the interests protected by the Fourth Amendment,⁷⁴ and for 80 years focused its Fourth Amendment jurisprudence on whether a search required government officials to trespass on private property. In *Olmstead v United States*,⁷⁵ for example, five of the nine justices found that wiretapping of telephone wires by federal officials did not constitute a search or seizure since there had been no physical trespass and nothing tangible had been taken.

In 1967, the Court decided *Katz v United States*,⁷⁶ a case involving the constitutionality of federal authorities' use of an electronic listening device attached to the outside of a telephone booth used by Charles Katz, whom the authorities suspected of violating gambling laws. The Court found that this method of gathering evidence infringed on Katz' Fourth Amendment rights, even though his property had not been invaded. The Court wrote that '[t]he Fourth Amendment protects people not places', and therefore applies to whatever one 'seeks to preserve as private, even in an area accessible to the public'.⁷⁷

In his concurrence, Justice Harlan introduced what was later to become the Court's test for what was 'private' within the meaning of the Fourth Amendment.⁷⁸ Justice Harlan wrote that the protected zone of Fourth Amendment privacy was defined by the individual's 'actual', subjective expectation of privacy, and the extent to which that expectation was 'one that society was prepared to recognize as "reasonable"'.⁷⁹ The Court adopted that test for determining what was 'private'

70 Id. at __, __.

71 The dissent argued that the majority overstated the access by others to prescriber data, citing state professional responsibility rules limiting disclosure of such data, the similarity of the exceptions in Vermont's law to exceptions in the major federal health privacy law (the Health Insurance Privacy and Accountability Act, or HIPAA), and the absence of record evidence indicating the widespread use of prescriber data for counterdetailing. Id. at __ (Breyer, J., dissenting).

72 Id. at __ (emphasis added).

73 U.S. Constitution amend. IV.

74 *Boyd v United States*, 116 U.S. 616, 625–26 (1886).

75 277 U.S. 438 (1928).

76 389 U.S. 347 (1967).

77 Id. at 351.

78 Id. at 360–61 (Harlan, J., concurring).

79 Id. at 361 (Harlan, J., concurring).

within the meaning of the Fourth Amendment in 1968 and has applied it with somewhat uneven results ever since.⁸⁰ The Court has found 'reasonable' expectations of privacy in homes,⁸¹ businesses,⁸² sealed luggage and packages,⁸³ and even drums of chemicals,⁸⁴ but no 'reasonable' expectations of privacy in voice or writing samples,⁸⁵ phone numbers,⁸⁶ conversations recorded by concealed microphones,⁸⁷ and automobile passenger compartments,⁸⁸ trunks (car boots),⁸⁹ and glove boxes.⁹⁰

The Supreme Court interprets the Fourth Amendment generally to require that searches be conducted only with a warrant issued by a court, even though this is not a requirement contained in the amendment itself.⁹¹ For a court to issue a warrant, the government must show 'probable cause' that a crime has been or is likely to be committed and that the information sought is germane to that crime.⁹² The Court also generally requires that the government provide the subject of a search with contemporaneous notice of the search.⁹³

The Fourth Amendment's protection, while considerable, is not absolute. The Supreme Court has carved out a number of exceptions to the warrant requirement; for example, warrants are not required to search or seize items in the 'plain view' of a law enforcement officer,⁹⁴ for searches that are conducted incidental to valid arrests,⁹⁵ for searches that serve 'special needs' unrelated to law enforcement (eg warrantless drug tests of high school athletes and railway employees),⁹⁶ and for searches specially authorized by the Attorney General or the President involving foreign threats of 'immediate and grave peril' to national security.⁹⁷

Moreover, the Supreme Court interprets the Fourth Amendment to apply only to the *collection* of information, not its *use*. Even if information is obtained in violation of the Fourth Amendment, the Supreme Court has consistently found that the Fourth Amendment imposes no independent duty on the government to refrain from using it. 'The Fourth Amendment contains

no provision expressly precluding the use of evidence obtained in violation of its commands, and an examination of its origin and purposes makes clear that the use of fruits of a past unlawful search or seizure "[works] no new Fourth Amendment wrong."⁹⁸

Under the Court's 'exclusionary rule', illegally seized data may still be used if the government agent acted in good faith,⁹⁹ to impeach a witness,¹⁰⁰ or in other settings in which the 'the officer committing the unconstitutional search or seizure' has 'no responsibility or duty to, or agreement with, the sovereign seeking to use the evidence'.¹⁰¹ The Court suppresses the use of information obtained in violation of the Fourth Amendment only when doing so would have deterred the conduct of the government employee who acted unconstitutionally when collecting the information. So, for example, the Court has allowed records illegally seized by criminal investigators to be used by tax investigators on the basis that restricting the subsequent use would not deter the original unconstitutional conduct.¹⁰² Protecting privacy is not a consideration. The Court wrote in 1974 that the exclusionary rule operates as 'a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than a personal constitutional right of the party aggrieved'.¹⁰³ If the Court finds no independent Fourth Amendment basis for restricting the use of illegally obtained information, it goes without saying that the Court does not apply the Fourth Amendment to restrict the use of lawfully obtained information. The Fourth Amendment today thus poses no limit on the government's use of lawfully seized records, and in the case of unlawfully seized material restricts its use only to the extent necessary to provide a deterrent for future illegal conduct

The Miller Exclusion of Third-Party Records

The Supreme Court held in 1976 in *United States v Miller*¹⁰⁴ that there can be no reasonable expectation of

80 *Terry v Ohio*, 392 U.S. 1 (1968).

81 *Camara v Municipal Court*, 387 U.S. 523 (1967).

82 *G.M. Leasing Corp. v United States*, 429 U.S. 338 (1977).

83 *United States v Chadwick*, 433 U.S. 1 (1977); *Arkansas v Sanders*, 442 U.S. 753 (1979); *Walter v United States*, 447 U.S. 649 (1980).

84 *United States v Knotts*, 460 U.S. 276 (1983).

85 *United States v Dionisio*, 410 U.S. 1 (1973).

86 *Smith v Maryland*, 442 U.S. 735 (1979).

87 *United States v White*, 401 U.S. 745 (1971).

88 *New York v Belton*, 453 U.S. 454 (1981).

89 *United States v Ross*, 456 U.S. 798 (1982).

90 *South Dakota v Opperman*, 428 U.S. 364 (1976).

91 Akihl Reed Amar, *The Constitution and Criminal Procedure* 3–4 (Yale University Press, New Haven, CT 1997).

92 68 *American Jurisprudence* 2nd edn, Searches and Seizures § 166 (1993).

93 *Richards v Wisconsin*, 520 U.S. 385 (1997).

94 *Coolidge v New Hampshire*, 403 U.S. 443 (1971).

95 *United States v Edwards*, 415 U.S. 800 (1974).

96 *Vernonia School Dist. 47J v Acton*, 515 U.S. 646 (1995); *Skinner v Railway Labor Executives' Assn.*, 489 U.S. 602 (1989); see also *City of Ontario v Quon*, 560 U.S. ___ (2010) (warrant not required for searches performed for non-investigatory work-related purposes or to investigate workplace misconduct).

97 68 *American Jurisprudence* 2nd edn, Searches and Seizures § 104 (1993).

98 *Leon*, 468 U.S. at 906 (quoting *United States v Calandra*, 414 U.S. 338, 354 (1974)).

99 *United States v Leon*, 468 U.S. 897 (1984).

100 *Walder v United States*, 347 U.S. 62 (1954).

101 *United States v Janis*, 428 U.S. 433, 455 (1975).

102 *Id.*

103 *Calandra*, 414 U.S. at 354.

104 *United States v Miller*, 425 U.S. 435 (1976).

privacy in information shared with a third party. The case involved cancelled checks, to which, the Court noted, ‘respondent can assert neither ownership nor possession.’¹⁰⁵ Such documents ‘contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business,’¹⁰⁶ and therefore the Court found that the Fourth Amendment is not implicated when the government sought access to them:

The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.¹⁰⁷

The Court’s decision in *Miller* is remarkably sweeping. The bank did not just happen to be holding the records the government sought. Instead, the Bank Secrecy Act required (and continues to require) banks to maintain a copy of every customer check and deposit for six years or longer.¹⁰⁸ The government thus compelled the bank to store the information, and then sought the information from the bank on the basis that since the bank held the data, there could not be any reasonable expectation of privacy and the Fourth Amendment therefore did not apply.¹⁰⁹ The Supreme Court was not troubled by this apparent end-run around the Fourth Amendment: ‘even if the banks could be said to have been acting solely as Government agents in transcribing the necessary information and complying without protest with the requirements of the subpoenas, there would be no intrusion upon the depositors’ Fourth Amendment rights.’¹¹⁰

The Court reinforced its holding in *Miller* in the 1979 case of *Smith v Maryland*, involving information about (as opposed to the content of) telephone calls.¹¹¹ The Supreme Court found that the Fourth Amendment is inapplicable to telecommunications ‘attributes’ (eg the number dialled, the time the call was placed, the duration of the call, etc.), because that information is

necessarily conveyed to, or observable by, third parties involved in connecting the call.¹¹² ‘[T]elephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes.’¹¹³

As a result, under the Fourth Amendment, the use of ‘pen registers’ (to record out-going call information) and ‘trap and trace’ devices (to record in-coming call information) does not require a warrant because they only collect information about the call that is necessarily disclosed to others.¹¹⁴ As with information disclosed to financial institutions,¹¹⁵ Congress reacted to the Supreme Court’s decision by creating modest statutory requirements applicable to pen registers,¹¹⁶ but the Constitution does not apply.

While the *Miller* third-party doctrine and its binary view of privacy have never been overruled or even questioned by a majority of the Court and have generally been followed by lower courts, the Supreme Court has declined to apply the doctrine in at least one case in which the Court found extensive and routine involvement of law enforcement in the design and administration of the third party’s collection of data. In *Ferguson v Charleston*,¹¹⁷ the Court held that a hospital drug-screening program for pregnant women that provided the results to local police without the women’s consent, in order to use threats of prosecution to prompt them to seek counselling and treatment, violated the Fourth Amendment. Justice Scalia dissented, noting: ‘Until today, we have never held—or even suggested—that material which a person voluntarily entrusts to someone else cannot be given by that person to the police, and used for whatever evidence it may contain.’¹¹⁸

In *City of Ontario v Quon*, the Court assumed that city police officers retained a reasonable expectation of privacy in text messages sent via employer-provided pagers, notwithstanding the fact that the contents of the messages were stored on a third-party provider’s (rather than the city’s) servers.¹¹⁹ The Court found that

105 Id. at 440.

106 Id. at 442.

107 Id. at 443 (citation omitted).

108 12 U.S.C. § 1829b(d); see 425 U.S. at 436; *California Bankers Assn. v Shultz*, 416 U.S. 21 (1974).

109 425 U.S. at 443.

110 Id. at 444.

111 442 U.S. 735 (1979).

112 Id. at 743.

113 Id.

114 *Smith v Maryland*, 442 U.S. 735, 742 (1979).

115 Right to Financial Privacy Act, 12 U.S.C. §§ 3401–3422.

116 18 U.S.C. §§ 3121, 1841.

117 532 U.S. 67 (2001).

118 Id. at 95 (Scalia, J., dissenting).

119 560 U.S. at ____.

the city's review of transcripts of such messages, supplied by the third-party provider upon request, was performed for legitimate, non-investigatory work-related purposes, was reasonable in scope, and thus was constitutional.¹²⁰ While noting that the messages were stored by the third party and not the city, the Court made no mention of *Miller* or *Smith* and undertook no analysis of any potential application of the third-party doctrine.¹²¹ Accordingly, it is difficult to deduce any impact on the doctrine from this case, including whether the Court might draw a line between government access to communication contents, which *Quon* involved, and access to communications attributes (*Smith*) or records the specific contents of which are necessary to the third party's business (*Miller*).¹²²

In the absence of such doctrinal limits, advances in technologies, and the development of new products and services in response to those changes, have significantly expanded the scope of the *Miller* exclusion of records held by third parties from the protection of the Fourth Amendment. Today there are vastly more personal data in the hands of third parties, they are far more revealing, and they are much more readily accessible than was the case in the 1970s. Moreover, for the first time, the government has the practical ability to exploit huge data sets. As a result, the scope of the *Miller* decision has been greatly expanded and the balance between the government's power to obtain personal data and the privacy rights of individuals substantially altered.

United States v Jones

One of the Supreme Court's most recent and significant Fourth Amendment cases, *United States v Jones*,¹²³ has challenged established Fourth Amendment privacy jurisprudence. Four justices of the Court (Scalia, Roberts, Kennedy, and Thomas), joined by Justice Sotomayor, reinterpreted *Katz* to find that the Fourth Amendment protects both people *and* places. The Court found that attaching a GPS device to the bumper of a suspect's car without a warrant constituted an unlawful search irrespective of any expectations of privacy because the government's action constituted a

trespass to private property. The Court wrote that 'the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test'.¹²⁴

While one could argue that the Court's resurrection of common-law trespass as an independent basis for invoking the Fourth Amendment—after 45 years of reliance on the *Katz* standard—worked an expansion of privacy rights, four concurring justices (Alito, Ginsburg, Breyer, and Kagan) argued that the majority's focus on trespass obscured the real privacy violation by the government: '[T]he Court's reasoning largely disregards what is really important (the use of a GPS for the purpose of long-term tracking) and instead attaches great significance to something that most would view as relatively minor (attaching to the bottom of a car a small, light object that does not interfere in any way with the car's operation)'.¹²⁵ This, the justices argue, is particularly problematic in the modern age when around-the-clock monitoring of a vehicle's location can be accomplished by activating the vehicle's stolen vehicle detection system or tracking one of the occupant's cell phones.¹²⁶

Justice Sotomayor wrote a separate concurrence in which she argued that it might be time for the Court to revisit *Miller* and the third-party doctrine:

More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.¹²⁷

Freedom of Information Act

Not all of the Supreme Court's privacy jurisprudence addresses constitutional issues. The federal Freedom of Information Act (FOIA) permits 'any person' to obtain access to all federal 'agency records', subject to nine

120 *Id.* at __. The Court declined to decide whether 'operational realities' might limit a government employee's reasonable expectation of privacy in communications on employer-issued devices, but nonetheless discussed in dicta some of the factors that it would have to consider if it undertook that inquiry; notably, the storage of such communications with a third party provider was not among the factors mentioned.

121 The Court held that any violation of statutory privacy protections (under the Stored Communications Act, 18 U.S.C. 2701 et seq.) by the provider in giving the city the text message contents upon request, did not invalidate the city's otherwise reasonable search. *Id.* at __.

122 While the city, and not individual personnel, made the decision to use the third-party provider, arguably this has no bearing on the potential application of the doctrine, since the storage of personal information with a third party in *Miller* and *Smith* was no less involuntary, from a practical standpoint.

123 __ U.S. __, 2012 U.S. LEXIS 1063.

124 *Id.* at __ (emphasis in original).

125 *Id.* at __ (Alito, J., concurring).

126 *Id.* at __.

127 *Id.* at __ (Sotomayor, J., concurring).

enumerated exemptions.¹²⁸ Two of the nine exemptions are designed to protect privacy: Exemption 6 precludes disclosure of ‘personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of privacy’, and Exemption 7(c) bans release of ‘records or information compiled for law enforcement purposes [which] . . . could reasonably be expected to constitute an unwarranted invasion of privacy.’¹²⁹

The Supreme Court has decided cases interpreting the extent of both exemptions and, in the process, of ‘privacy’. In 1989, the Court decided *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*,¹³⁰ which involved press access to law enforcement rap sheets. The press argued that because the information in an individual’s rap sheet was compiled from local, publically available law enforcement and court records, the individual could not assert any privacy right. The Court disagreed, writing: ‘We reject respondents’ cramped notion of personal privacy.’¹³¹

The Court wrote, ‘both the common law and the literal understandings of privacy encompass the individual’s control of information concerning his or her person. In an organized society, there are few facts that are not at one time or another divulged to another.’¹³² According to the Court, previous disclosure does not automatically remove the privacy interest. Instead, ‘the extent of the protection accorded a privacy right at common law rested in part on the degree of dissemination of the allegedly private fact and the extent to which the passage of time rendered it private.’¹³³ The Court went on to note that according to ‘Webster’s initial definition, information may be classified as “private” if it is “intended for or restricted to the use of a particular person or group or class of persons: not freely available to the public”.’¹³⁴

Based on this nuanced interpretation of privacy, the Court found that FBI rap sheets, even if they contain only material that is held by local law enforcement agencies and courts and that material has been made public, are nevertheless ‘private’ within the meaning of

FOIA because of the passage of time, the limited purposes motivating that disclosure, and the fact that rap sheets aggregate otherwise disparate pieces of information.

The Court in *Reporter’s Committee* quoted approvingly from a speech by then-Justice William Rehnquist: ‘In sum, the fact that “an event is not wholly ‘private’ does not mean that an individual has no interest in limiting disclosure or dissemination of the information”.’¹³⁵ The Court concluded its analysis: ‘The privacy interest in a rap sheet is substantial. The substantial character of that interest is affected by the fact that in today’s society the computer can accumulate and store information that would otherwise have surely been forgotten long before a person attains age 80, when the FBI’s rap sheets are discarded.’¹³⁶

Five years later, the Supreme Court relied on its broad definition of privacy from *Reporter’s Committee* in a case involving FOIA’s other privacy exemption, Exemption 6, which applies to ‘personnel and medical files and similar files the disclosure of which would constitute a clearly un-warranted invasion of personal privacy.’¹³⁷ In *United States Department of Defense v. Federal Labor Relations Authority*,¹³⁸ the Court was faced with a request by two unions for certain federal employees’ home addresses.

Addressing the issue of whether information as public as home addresses could ever be considered private, the Court wrote: ‘It is true that home addresses often are publicly available through sources such as telephone directories and voter registration lists, but “in an organized society, there are few facts that are not at one time or another divulged to another.”’¹³⁹ The Court noted that the ‘individual’s interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form.’¹⁴⁰ The Court found that ‘it is clear that [individuals] have some nontrivial privacy interest in nondisclosure.’¹⁴¹ The Court, therefore, found that Exemption 6 prohibited the disclosure of federal employees’ addresses.

128 5 U.S.C. § 552 (1997).

129 Id. § 552(b)(6)–(7)(C).

130 489 U.S. 749 (1989).

131 Id. at 763.

132 Id.

133 Id.

134 Id. at 763–64.

135 Id. at 710–71 (quoting William Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement?*, Nelson Timothy Stephens Lectures, University of Kansas Law School, pt. 1, p. 13 (Sept. 26–27, 1974)).

136 Id. at 771. In *National Archives and Records Administration v. Favish*, 541 U.S. 157 (2004), the Supreme Court further expanded its understanding of the ‘privacy’ at issue in FOIA cases, by extending Exemption 7(c) to family members of an individual who committed suicide.

137 5 U.S.C. § 552(b)(6).

138 510 U.S. 487 (1994).

139 Id. at 550 (quoting *Reporter’s Committee*, 489 U.S. at 763).

140 Id.

141 Id. at 501.

Assessment

It is not surprising that many commentators have considered the Supreme Court's privacy jurisprudence to be confused and disjointed. The Court not only uses the term in a variety of different settings, but has defined it to have at least three distinct meanings.

The first, which the Court has described variously as a 'right of personal privacy' or 'areas or zones of privacy',¹⁴² is constitutionally protected to the extent the right can be deemed to involve decisions whose personal nature is "fundamental" or "implicit in the concept of ordered liberty".¹⁴³ The Court has found fundamental rights of private decision making concerning marriage, procreation, contraception, consensual sexual relations, family relationships, child rearing, and education.¹⁴⁴ As noted above, this right generally does not implicate information privacy, except in limited contexts involving compelled disclosures (both to and from the pregnant woman) surrounding abortion.

The second meaning of privacy comes from the Court's Fourth Amendment jurisprudence. In this setting, the Court has provided a specific definition: whatever one 'seeks to preserve as private, even in an area accessible to the public',¹⁴⁵ provided that the individual has an 'actual, subjective expectation of privacy, and that expectation is 'one that society was prepared to recognize as "reasonable"'.¹⁴⁶ The Court has crafted many exceptions to this right, the most significant being that for information to be treated as private, it must not have been disclosed to, or be held by, a third party.¹⁴⁷ As a result, this understanding of privacy is essentially binary: information is either not disclosed and therefore private or it has been disclosed and therefore is not private. And this constitutional understanding of privacy is solely concerned with the collection of data, not with its retention, use or sharing.

The Court describes its third meaning of privacy in the constitutional context as 'the individual interest in avoiding disclosure of personal matters...'.¹⁴⁸ The Court has explicitly noted that information that the government constitutionally may require an individual to disclose for one purpose, may nevertheless remain sensitive and subject to privacy protections. Many legitimate government activities 'all require the orderly

preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures'.¹⁴⁹ Despite the fact that the information has been disclosed to, and is held by, someone other than the data subject, 'in some circumstances that duty [to avoid unwarranted disclosures] arguably has its roots in the Constitution'.¹⁵⁰ Nevertheless, this interest in non-disclosure was recognized in *Whalen*, a case upholding the compelled disclosure of prescription information, and has not yet invoked strict scrutiny by the Court of a government data-related activity.

In the statutory context, the Court has used this third meaning of privacy to block disclosure under FOIA. Repeatedly, the Court has found that even though information has been disclosed to and is held by third parties, this does not eliminate the existence of a lawfully protected privacy interest. '[T]he fact that "an event is not wholly 'private' does not mean that an individual has no interest in limiting disclosure or dissemination of the information"'.¹⁵¹ This is a far more subtle view of privacy, in which privacy is measured on a spectrum, rather than the binary view of privacy that the Court applies in its Fourth Amendment jurisprudence.

The fact that there is inconsistency in the Court's privacy jurisprudence is not surprising. In fact, the Court itself noted in *Reporter's Committee* that the 'question of the statutory meaning of privacy under the FOIA is, of course, not the same as the question whether a tort action might lie for invasion of privacy or the question whether an individual's interest in privacy is protected by the Constitution'.¹⁵² However, the Court is inconsistent even within its constitutional privacy jurisprudence, employing the term in *Whalen* to mean something broad and subtle and requiring protection beyond mere collection limits, and in the Court's Fourth Amendment cases to refer to something that can be eliminated by disclosure, and requires no protection beyond collection limits.

Even more significant than the inconsistency, however, is that the meaning of privacy that the Court

142 *Roe v Wade*, 410 U.S. at 152.

143 *Id.* (quoting *Palko*, 302 U.S. at 325).

144 410 U.S. at 152–3; *Lawrence v Texas*, 539 U.S. 558.

145 *Katz*, 389 U.S. at 351.

146 *Id.* at 361 (Harlan, J., concurring); *Terry*, 392 U.S. 1.

147 *Miller*, 425 U.S. 435; *Smith*, 442 U.S. 735.

148 *Whalen*, 429 U.S. at 599–600.

149 *Id.* at 605.

150 *Id.*

151 489 U.S. at 710–711 (quoting William Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement?*, Nelson Timothy Stephens Lectures, University of Kansas Law School, pt. 1, p. 13 (Sept. 26–27, 1974)).

152 489 U.S. at 763 n.13.

has so far articulated in its Fourth Amendment jurisprudence is inconsistent with popular perceptions about the meaning of privacy and renders the Fourth Amendment impotent to protect against government intrusions into vast collections of personal information, given the extraordinary increase in both the volume and sensitivity of information about individuals necessarily held by third parties.

Professor Daniel Solove writes: 'We are becoming a society of records, and these records are not held by us, but by third parties.'¹⁵³ Thanks to the proliferation of digital technologies and networks such as the internet, and tremendous advances in the capacity of storage devices and parallel decreases in their cost and physical size, those records are linked and shared more widely and stored far longer than ever before, often without the individual consumer's knowledge or consent.¹⁵⁴ This is especially true as more activities move online, where merchants record data not only on what individuals buy and how we pay for our

purchases, but also on every detail of what we look at, what we search for, how we navigate through web sites, and with whom we communicate.

The *Miller* exclusion from the Fourth Amendment of information disclosed to third parties means that all of this information, no matter how sensitive or how revealing of a person's health, finances, tastes, or convictions, is available to the government without constitutional limit. The government's demand need not be reasonable, no warrant is necessary, and no judicial authorization or oversight is required. *Jones* raises the possibility that at least some members of the Court recognize the impact of technological change on the Fourth Amendment's protection for privacy, and may even be willing to revisit *Miller*, but the outcome is far from certain.

doi:10.1093/idpl/ips024

Advance Access Publication 26 September 2012

153 Daniel J. Solove, 'Digital Dossiers and the Dissipation of Fourth Amendment Privacy', (2002) 75 *Southern California Law Review* 1083, 1089.

154 Id.; James X. Dempsey and Lara M. Flint, 'Commercial Data and National Security', (2004) 72 *George Washington Law Review* 1459; Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (Vintage Books, New York 2001).